К. С. Пермякова, С. В. Бегичева
Уральский государственный экономический университет, г. Екатеринбург
УДК 004

REMOTE SERVICE SESSION HIJACKING T1563 — ПЕРЕХВАТ СЕАНСА УДАЛЕННОГО ОБСЛУЖИВАНИЯ

Аннотация. В данной статье приведено понятие сеанса удаленного обслуживания. Рассмотрен процесс перехвата сеанса удаленного обслуживания. Приведены последствия перехвата сеанса удаленного обслуживания. Рассмотрены способы предотвращения перехвата сеанса удаленного обслуживания.

Ключевые слова: сеанс удаленного обслуживания, перехват сеанса, безопасность при использовании сеансов, конфиденциальная информация.

Введение. Большинство людей ежедневно пользуются различными сайтами и порталами. Как только пользователь открывает сайт, начинается процесс взаимодействия двух информационных систем, который продолжается, пока пользователь не завершит его. Этот процесс называется сеансом информационного взаимодействия. Однако каждый сеанс сопряжен с определенным риском его перехвата. Данную тему в своих работах рассматривали Д. Е. Исаев [1], В. С. Попукайло и Е. А. Бугаенко [2].

Проблема исследования. При подключении к сайту или приложению через протокол HTTP сервис аутентифицирует пользователя, например, по логину и паролю, и только после этого открывает канал связи, предоставляя доступ. Однако сами HTTP-подключения не отслеживают состояние данных, поэтому каждое действие пользователя воспринимается как отдельное от других. Если полагаться исключительно на протокол HTTP, необходимо будет вводить учетные данные каждый раз при переходе на новую страницу или при выполнении других действий на сайте. Так пользователь может столкнуться с проблемой перехвата сеанса и кражи личных данных.

Материалы и методы. Для решения этой проблемы существуют сеансы. Они создаются после успешного ввода учетных данных на сервере, на котором расположен сайт или приложение. Благодаря сеансу используемые сайт или приложение запоминают начальные аутентификационные данные. Пользователь остается в системе до тех пор, пока сеанс открыт, и завершает его, когда выходит из системы. Иногда сеансы закрываются автоматически после некоторого периода бездействия пользователя.

При создании сеанса многие сервисы генерируют уникальный идентификатор сеанса, представляющий собой строку из цифр и букв, которая хранится во временном файле сеанса, например, в cookie или в ссылках. Некоторые сервисы шифруют идентификаторы сеансов. Часто идентификаторы содержат данные, легко доступные для узнавания, такие как IP-адрес пользователя.

Перехват сеанса — это атака, в процессе которой злоумышленник перехватывает контроль над сеансом пользователя. Также эта атака известна как перехват файлов cookie или перехват TCP. Атака может произойти в момент, когда человек выбирает товар в интернет-магазине или проверяет баланс банковского счета. Обычно злоумышленники перехватывают сеансы браузера и веб-приложений, стремясь получить доступ к персональным данным и паролям [2].

Процесс перехвата пользовательских сеансов происходит следующим образом:

1. Пользователь авторизуется в своей учетной записи, например, в приложении или портале. При этом браузер создает временный файл сеанса — cookie. Этот файл содержит информацию о пользователе, которая позволяет ему оставаться в системе, а также отслеживает его активность в течение сеанса. Файл cookie сеанса сохраняется до выхода пользователя из учетной записи либо до автоматического завершения сеанса после заданного на сервере периода бездействия.

2. Злоумышленник получает доступ к активному сеансу пользователя. Преступники применяют различные методы перехвата сеансов. Например, они могут украсть файл cookie, найти в нем идентификатор сеанса, также известный как ключ сеанса, и использовать эту информацию для перехвата сеанса. Получив идентификатор, злоумышленник может без оставления следов вмешаться в сеанс.

3. Начинает действовать атака. Авторизированный пользователь продолжает использовать интернет, однако злоумышленник использует его активный сеанс в своих целях. Он может красть деньги со счета пользователя, совершать покупки, извлекать личные данные и использовать их в дальнейшем, а также шифровать важную информацию и потребовать выкуп за ее расшифровку.

Выдавая себя за авторизованного пользователя, злоумышленник получает несанкционированный доступ к защищенным учетным записям и содержащимся в них данным [1]. Такие атаки могут привести к серьезным последствиям для безопасности ресурса. Защищая себя от перехвата сеансов, можно предотвратить следующие угрозы:

– Кража личных данных. Злоумышленники, получив несанкционированный доступ к личной информации, хранящейся в учетных записях, могут использовать ее за пределами скомпрометированного веб-сайта или приложения.

– Финансовые махинации. Захват сеанса позволяет злоумышленникам осуществлять транзакции от имени пользователя, такие как вывод денежных средств с банковских счетов или покупки на веб-сайтах, где хранятся данные банковских карт.

– Инфицирование вредоносным программным обеспечением (далее — ПО). Используя идентификатор сеанса, злоумышленники могут заразить устройство пользователя вредоносным программным обеспечением, получить доступ к компьютеру и похитить ценные данные.

– Атаки типа DoS — отказ в обслуживании. После захвата сеанса пользователя злоумышленники могут запустить атаку DoS на веб-сайт или сервер, к которому пользователь подключен. Это может привести к сбоям в работе сервиса или временной недоступности веб-ресурса.

– Доступ к другим системам через службу единого входа (SSO). С помощью SSO злоумышленники могут получить несанкционированный доступ к нескольким службам, используемым пользователем, что увеличивает риск атак с перехватом сеанса. Это особенно актуально для организаций, использующих технологию SSO для повышения производительности сотрудников. Необходимо помнить, что надежность систем с надежными методами аутентификации и непредсказуемыми cookie-сеансами, например, систем обработки финансовой и конфиденциальной информации, остается на уровне ее самого слабого звена.

Результаты. Для того, чтобы предотвратить перехват сеанса стоит следовать нескольким правилам:

– Стоит избегать использования открытых Wi-Fi сетей. Не нужно проводить финансовые операции или входить в личные аккаунты через общедоступные сети, где злоумышленникам проще получить доступ к данным.

– Использовать VPN. Если все же появляется необходимость воспользоваться общественной сетью Wi-Fi, то следует использовать VPN для повышения безопасности и шифрования данных, передаваемых между устройством и сетью.

– Следует проявлять бдительность по отношения к фишингу. Открытие подозрительных ссылок может привести к установке вредоносного ПО на устройство или к переходу на фальшивые сайты.

– Использовать только проверенные сайты. Например, сайты с HTTPS протоколом являются надежными и безопасными, поэтому их использование минимизирует риск перехвата сеанса.

– Устанавливать антивирусное программное обеспечение. После установка необходимо также регулярно обновлять антивирусного программного обеспечения. Это поможет защитить устройство от вирусов, вредоносного ПО и программ для перехвата сеансов.

Заключение. Таким образом, безопасность при использовании сеансов играет важную роль в защите конфиденциальной информации пользователей. Прибегая ко всем вышеперечисленным мерам, пользователь сможет усилить защиту данных от перехвата сеанса удаленного обслуживания и сделать использование удаленных сервисов более безопасным и надежным.

СПИСОК ЛИТЕРАТУРЫ

1. Исаев Д Е. Основные проблемы безопасности корпоративных сетей передачи данных / Д.Е. Исаев // Инновационная траектория развития современной науки: становление, развитие, прогнозы: сборник статей VI Международной научно-практической конференции, Петрозаводск, 17 июня 2021 года. — Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская Ирина Игоревна), 2021. — С. 82-89. — EDN GMFRQO.
2. Попукайло В.С., Бугаенко Е.А. Анализ угроз и источников возникновения сетевых уязвимостей // Актуальные проблемы науки и образования в условиях современных вызовов. — 2023. — С. 73-78.